Sophos lanza 4 desarrollos en IA abiertos a la industria

CIUDAD DE MÉXICO. 15 de diciembre de 2020.- Sophos, líder mundial en ciberseguridad de última generación, anunció el lanzamiento de **cuatro nuevos desarrollos de código abierto en inteligencia artificial (IA)**, que ayudarán a ampliar las capacidades de los sistemas de seguridad de la industria contra los ataques cibernéticos.

Los desarrollos incluyen nuevos conjuntos de datos, herramientas y metodologías diseñadas para promover la colaboración entre empresas y la innovación en seguridad.

Estos lanzamientos aceleran uno de los objetivos clave de Sophos: **abrir sus avances en la ciencia de datos y hacer que el uso de IA en la ciberseguridad sea más transparente,** con el fin de proteger mejor a las organizaciones contra todas las amenazas existentes.

Si bien en otras industrias es común compartir metodologías y hallazgos de IA, la ciberseguridad se ha quedado rezagada en este esfuerzo, lo que ha resultado en poca claridad sobre cómo esta tecnología ayuda a brindar protección contra ciberamenazas.

Sophos y su equipo de científicos de datos de SophosAI están iniciando un cambio hacia la apertura en inteligencia artificial, de modo que los gerentes de TI, analistas de seguridad, directores financieros y demás personal dentro de las compañías tomen decisiones basadas en datos e información de valor.

"*Con esta nueva iniciativa de SophosAI de abrir su investigación, podemos ayudar a influir en cómo se posiciona y se discute el uso de la inteligencia Artificial en la ciberseguridad hacia el futuro. Las actuales afirmaciones opacas y cautelosas sobre las capacidades y la eficacia de esta tecnología en las soluciones de seguridad hacen que sea difícil o casi imposible para las empresas comprender su uso al proteger los sistemas de sus organizaciones. Esto lleva al escepticismo de los encargados de TI, creando un escenario a contracorriente para el progreso de esta tecnología en el sector de ciberseguridad, pese a que existen grandes avances"*, indicó Joe Levy, director de Tecnología de Sophos.

"Corregir esto a través de mecanismos y estándares ya establecidos no sucederá lo suficientemente rápido. Por el contrario, se requiere de un esfuerzo dentro de la industria de generar un conjunto de nuevas prácticas que generarán un avance, mismas que deben ser abiertas y transparentes para todos", añadió.

No es una exageración decir que este cambio resulta muy relevante en cuanto al beneficio que puede generar a la ciberseguridad, dado el inmenso potencial de la inteligencia artificial como tecnología.

Las evidencias de Sophos muestran que los equipos de seguridad enfrentan adversarios cada vez más sofisticados, quienes lanzan campañas de falsificación tipo Business Email Compromise (BCE) cada vez más agresivas y altamente desarrolladas, así como generando nuevos ataques de propagación de ransomware.

Las defensas ante ese tipo de ciberataques deben ser más escalables y efectivas, por lo que requieren de IA, cuya apertura entre quienes la aplican para abordar estas amenazas estimula la innovación y los descubrimientos sobre el uso de esta tecnología en materia de seguridad, lo que impulsa a toda la industria.

Las herramientas y metodologías lanzadas por Sophos en este rubro son:

- **SOREL-20M para acelerar la investigación de detección de malware**

SOREL-20M es un proyecto conjunto entre SophosAI y ReversingLabs que consiste en **datos a escala de producción con etiquetas y características para 20 millones de archivos** en formato Windows Portable Executable (PE).

Incluye 10 millones de muestras de *malware* deshabitado, disponibles para su descarga, con el fin de investigar y acelerar las mejoras de seguridad en toda la industria. Este es el **primer conjunto de datos de investigación de *malware* a escala de producción disponible para el público en general,** con un etiquetado de muestras y metadatos muy relevantes para la seguridad.

- **Método de protección contra la suplantación de identidad impulsado por IA**

La protección contra suplantación de identidad de SophosAI está diseñada contra ataques de *phishing*, en los que se suplanta la identidad de personas y/o empresas para engañar a los destinatarios y hacer que sigan algunos pasos en beneficio del atacante.

Esta nueva protección **compara las direcciones y nombres que utilizan quienes envían estos correos electrónicos con los títulos de ejecutivos de alto nivel de las empresas**, que son los que tienen más probabilidades de ser falsificados en un ataque, tales como un CEO, CFO o presidente.

Con ese análisis, la tecnología **‘marca’ los correos que parecen sospechosos y alerta a los colaboradores al respecto.** Sophos cuenta con una muestra de millones de correos electrónicos de ataque y ha abierto este método de protección, que ha sido debatido en Defcon 28 y en un artículo de Arxiv.

- **Epidemiología digital para encontrar *malware***

SophosAI también ha creado un conjunto de **modelos estadísticos inspirados en la epidemiología** para estimar la prevalencia de infecciones de *malware*, lo que permite a Sophos estimar y, a su vez, tener una mejor oportunidad de encontrar las amenazas que se ocultan como ‘agujas en pajar’ en forma de archivos (PE).

Como pionera, SophosAI ha puesto a disposición del público este método que **ayuda a detectar *malware* que puede pasar por alto o ser clasificado incorrectamente como archivos legítimos**, además de "*malware* futuro" que los atacantes están desarrollando. El modelo está diseñado para ser extensible a otras clases de archivos y artefactos del sistema de información.

- **YaraML: herramientas de generación automática de firmas**

La generación de firmas para la detección de familias de *malware* es un proceso manual y laborioso. A lo largo de los años, los investigadores han propuesto una variedad de métodos automáticos de generación de firmas, la mayoría de los cuales no han tenido la adopción adecuada porque tienen un rendimiento inferior a los métodos manuales.

SophosAI ha desarrollado un nuevo proceso llamado **YaraML**, que es significativamente diferente a las opciones anteriores al adoptar un enfoque del problema basado en IA.

Este método **utiliza modelos de aprendizaje automático de capacidad industrial, como los utilizados en productos de seguridad comercial,** en lenguajes de firmas, lo que permite que la IA las "escriba". Esto demuestra ser mucho más efectivo que los enfoques anteriores y representa un gran avance para la comunidad de ciberseguridad. **SophosAI tiene el método YaraML en código abierto.**

Estos cuatro avances son los más recientes de **SophosAI, que funciona como una incubadora de empresas emergentes, pero con los recursos de una empresa global** de casi mil millones de dólares, incluidos SophosLabs, Sophos Managed Threat Response y cientos de miles de clientes.

Otra ventaja es que puede agregar nueva tecnología directamente a los productos de la firma. Este modelo permite a Sophos reaccionar rápidamente a las necesidades del mercado, predecir hacia dónde debe dirigirse la industria y promover la apertura para una mayor colaboración e innovación en el sector de la ciberseguridad, lo cual es esencial para desarrollar defensas contra adversarios que evolucionan rápidamente.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos

ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/